Back to Basics June 12

The CCH has seen a few instances recently where published histories on the outside that deal with World War II cryptology have used WW II cryptologic terminology incorrectly or made other erroneous statements about the wartime effort. We decided it would be a good idea to lay out some terminology and basic facts for reference.

If all this sounds like a primer, well, yes, it is. But we hope it is also an interesting primer.

Both the United States and Great Britain had intensive cryptanalytic efforts before World War II, and both enjoyed a measure of success. Although both countries worked a variety of targets, the British concentrated on German cryptosystems, and the U.S. on Japanese systems. Each gave a covername to the systems they sought to solve, and, when successful against an adversary's system, they applied a different covername to the results of the cryptanalysis.

The Americans and British began cautious sharing in early 1941 of what the British called Signals Intelligence (SIGINT) and U.S. officials called Communications Intelligence (COMINT). Over the course of the war, just as the two nations grew closer in military operations, their cryptologic organizations greatly increased cooperation.

Both countries had a covername that was applied to the information derived from exploiting a foreign cryptosystem. This had a double purpose; it would help keep the intelligence information within carefully controlled distribution system, and it would alert the reader to the fact that the intelligence had been obtained through an extremely fragile process and could only be discussed with others who held the proper clearances for that kind of intelligence.

The American coverword for COMINT was MAGIC. The British called the product of cryptanalysis of high-grade systems ULTRA. As binational cooperation strengthened during the war, the U.S. also adopted ULTRA as its codeword—

except that MAGIC continued as a codeword for certain specialized diplomatic product.

The ENIGMA

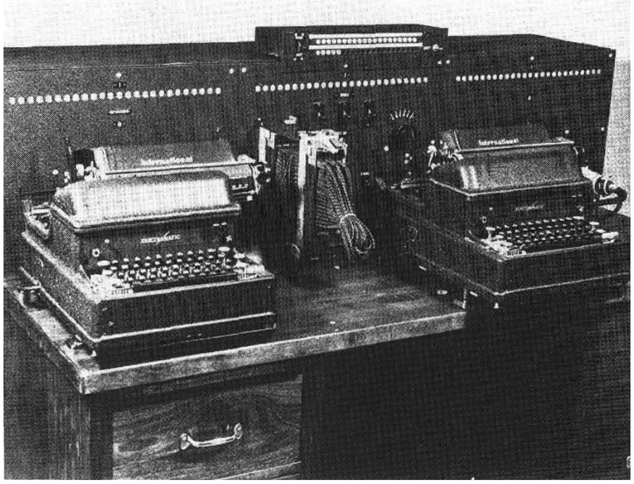
The most widespread German system exploited by the Allies was the ENIGMA machine. “ENIGMA” was the actual name of an electromechanical device that used rotating disks and plugs in a plug board to scramble individual letters. The ENIGMA had been developed for commercial use by banks and businesses, but was adopted by the German military, improved, and widely used.

The initial solution of ENIGMA-based messages was achieved by the Polish Cipher Bureau in the mid-1930s; the cryptanalytic team was led by a mathematician who had a degree from a German university, Marian Rejewski. The first solution was done by hand, but the Polish analysts developed a machine to speed up the process; they called this device a *bomba*. It became better known by its French name, *bombe*.

The Poles shared their solution of the ENIGMA with the British, whose cryptologic organization was known as the Government Code & Cypher School (GC&CS), a deliberately misleading name. The British improved the *bombe*, making it faster and more efficient. Among those involved in this effort were Alan Turing and Gordon Welchman, also mathematicians. The British established a highly effective system for collecting enemy signals, processing them, and distributing product worldwide. This has come to be known as the ULTRA system, and the Americans modeled much of their own SIGINT system on it.

The Germans used other cipher systems than the ENIGMA, some less sophisticated for front-line use, and some more complex, for use by the higher leadership. One such device was known to the British as TUNNY. This was solved in theory by the British, capitalizing on a mistake by a German machine operator. In order to exploit the TUNNY in a timely way to get intelligence, the British developed an analytic machine called the COLOSSUS, which many argue was the world's first operational computer.

In the 1930s, the U.S. Army's Signal Intelligence Service solved a machine-generated Japanese diplomatic cryptosystem. The Americans nicknamed the machine PURPLE. Decrypts of PURPLE traffic gave insights into Japanese foreign policy in the period before the Japanese attack on Hawaii in December 1941. After the attack, which, of course, ruptured diplomatic relations between Japan and the United States, PURPLE proved even more useful than it had before the war. The United States decrypted reports from the Japanese ambassador in Berlin, and the reports often gave detailed inside information about the German war effort.



PURPLE *Analog*

The original solution for PURPLE was a team effort. William Friedman was the overall supervisor, but the analytic work was led by Frank Rowlett. The initial solution of the Japanese system was made possible when mathematician Genevieve Grotjean discovered some statistical anomalies. Once the system was solved, an engineer named Leo Rosen fabricated a device known as the PURPLE Analog, which provided rapid decryption of individual messages.

A recent popular book about a famous U.S. female cryptanalyst attributed the intelligence that was important in the Battle of Midway in June 1942 to the exploitation of PURPLE. This is not true. Read on.

In early 1942, after the Japanese surprise attack on Hawaii, the U.S. Navy's cryptologic organization, OP-20-G, broke into the mainline Japanese Navy code (actually, an enciphered code) that the Americans called JN-25. The ability to exploit this system gave the U.S. Navy inside information about the order of battle and operations of its enemy in the Pacific. Exploitation of this system was the source of the secret intelligence that greatly supported U.S. Navy decision makers in the Battle of Midway.

The British cryptologic headquarters during World War II was Bletchley Park, a private estate acquired by the intelligence services just before hostilities broke out. Early in World War II, the American Army and Navy each acquired a former girls' school for their main cryptologic facility. The Army was at Arlington Hall Station, in northern Virginia, and the Navy at a facility on Ward Circle, where Nebraska and Massachusetts Avenues met in the District of Columbia.

This article was prompted by errors seen in some recent books, several of which are otherwise authentic. The cryptologic side of World War II was much more complex, but we must begin with the basics.

502 caption: photo 1 --- a German ENIGMA machine, open to expose the rotors and plugboard; photo 2 --- PURPLE Analog, a long metal box, with two typewriters